IN THE U.S. PATENT AND TRADEMARK OFFICE

U.S. Patent Application Serial No. 10/531,430 Confirmation No.: 8714

First Named Inventor: JEAL, DAVID

Filing Date: 10/04/2005

Art Unit: 2431

Examiner: HENNING, MATTHEW T

Docket No.: P08620US00/BAS

Customer No.: 881

DECLARATION OF CHARLES WILLIAM DEBNEY UNDER 37 C.F.R. 1.132

Commissioner for Patents
Alexandria, VA 22313-1450

I, Charles William Debney, declare and state as follows:

1. I reside at Prospect Lodge, Station Road, Kintbury, BERKSHIRE, RG17 9UP, UNITED KINGDOM.

2. I am one of the inventors listed in U.S. Patent Application No. 10/531,430 (hereinafter "our application"), which is a U.S. National Stage application of International Application No. PCT/GB03/04371, filed October 9, 2003, having a priority date claim of October 17, 2002.

3. I am presently employed as Head of Architecture & Innovation, Business Services, Vodafone Group PLC, (the assignee of U.S. Patent Application No. 10/531,430).

4. I received the degree of PhD. from the University of Southampton in 1982.

5. I have been active in the design, engineering, marketing and manufacturing of devices and methods of facilitating and authenticating transactions since 2001.

6. My experience also includes: extensive industrial experience in communications and software systems since 1984.

I am an active member of: Institution of Engineering and Technology (IET) and British Computing Society (BCS).

7. I am thus well familiar with the subject matter of the claims of the present application.

8. Our invention relates to the facilitation and authentication of transactions. In embodiments of the invention, transactions between a data processing apparatus (such as a personal computer), or a user thereof, and a (possibly remote) third party are facilitated and authenticated, and such facilitation and authentication may also involve the facilitation and authentication of a payment or data transfer to be made by or on behalf of the user to the third party. See: paragraph [0001] of our application, published as U.S. Patent Application Publication No. US 2006/0112275 A1.

9. A device according to our invention, for connection to a data processing apparatus, includes authentication storage means operatively coupled thereto for storing predetermined authentication information respective to a user. The authentication storage means is registered with a telecommunications system which includes authenticating means and for which the user has a telecommunications terminal. The device, when operatively coupled to the authentication storage means, is responsive to an input message for deriving a response dependent on the input message and on the authentication information for enabling the authenticating means to carry out

an authentication process via a communication link with the authenticating means in the telecommunications system whereby to authenticate a subsequent transaction by the user with the data processing apparatus and which involves use of the data carried by the authentication storage means. The predetermined authentication information stored by the authentication storage means corresponds to information which is used to authenticate the user registered with the telecommunications system in relation to use of that user's telecommunications terminal in the telecommunications system. However, the authentication process for authenticating the transaction by that user with the data processing apparatus does not require use of the user's telecommunications terminal nor does it require the telecommunications terminal to be actually authenticated by that information in relation to the telecommunications system. Further, the device controls access to the authentication information.

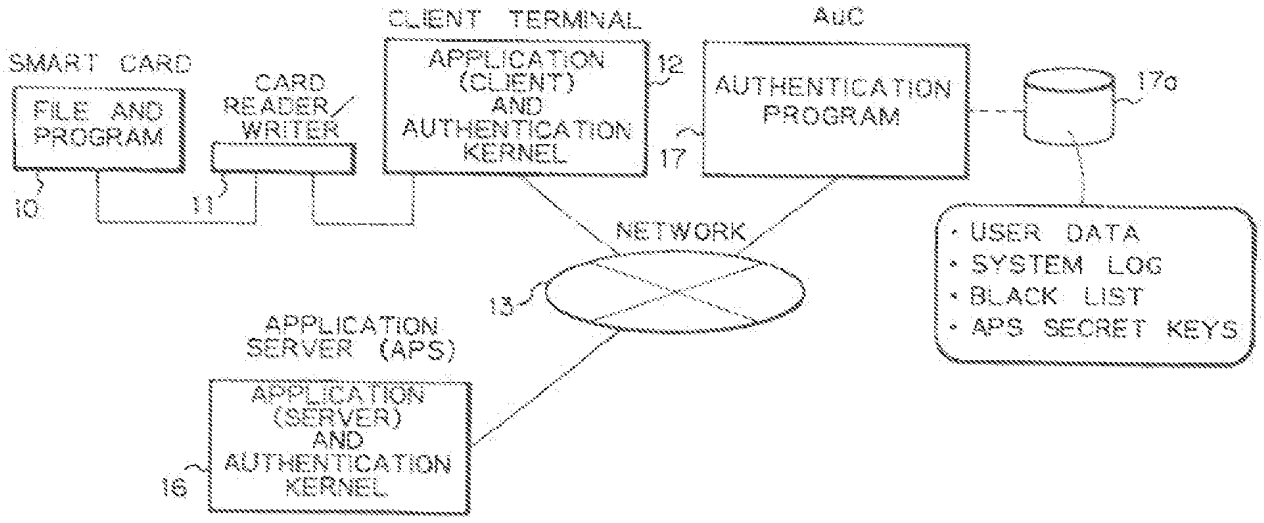
10. A method for authenticating a transaction with a data processing apparatus, according to our invention, has similar features to those described in the preceding paragraph.

11. In conjunction with this application, I have reviewed and am familiar with U.S. Patent No. 5,761,309, issued June 2, 1998 to Ohashi et al., entitled "AUTHENTICATION SYSTEM" (hereinafter "Ohashi").

12. FIG. 6 of Ohashi (reproduced below) is a block diagram schematically showing an embodiment of an authentication system of a purported invention (col. 11, lines 7-9). In the figure, reference numeral 10 denotes a smart card provided with a program and a file and possessed by each user, 11 denotes a card reader/writer for reading information from or writing information to the smart card 10, and 12 denotes a client terminal connected to the reader/writer

11, provided with client side application and authentication kernel, respectively (col. 11, lines 10-16).

Fig. 6



13. At column 12, lines 1-29, Ohashi states:

> For the card user, a PIN code has been previously defined, and this defined PIN code has been stored in the smart card 10. The user inputs his PIN code through the client terminal 12 into the smart card 10 so that coincidence between the input PIN code and one stored in the smart card 10 is checked. This check of the PIN code is executed by internal operation of the smart card 10. If PIN code input is successively failed three times, the smart card 10 permits no more access and thus the authentication procedure terminates. Since the memory in the smart card 10 is a nonvolatile storage, the number of the past successive PIN input failure will be held even if the power is off. This storage will be cleared if PIN code check is succeeded within successive three times inputs.
>
> After the smart card 10 is activated by local verification between the user and the smart card 10, authentication processes are carried out with following two phase sequence.
>
> A first phase is request and issuance of a user certificate. In this first phase, the user side (smart card 10) requests the AuC 17 to issue a certification information (user certificate) which verifies

> him. The issued user certificate which has a valid period is stored in the smart card 10. Prior to accessing the AuC 17, the user side (smart card 10 or client terminal 12) confirms the validity of the already obtained user certificate. As long as the user certificate is valid, the authentication processes can be jumped to a next second phase without accessing the AuC 17. This causes throughput in the AuC 17 to decrease.

14. I understand that the Examiner has characterized the passage of Ohashi at column 12, lines 1-29 as a disclosure of "enabling the authentication means to carry out an authentication process ... to authenticate a subsequent transaction by the user with the data processing apparatus ..." as recited in the claims of our application. However, this characterization is not accurate. Rather, the cited passage of Ohashi describes the conventional mechanism by which a client terminal (e.g., a telecommunication handset) checks that the user has input a PIN that matches the PIN stored on a smartcard/SIM. The scenario set out in Ohashi is thus entirely different than the subject matter of our invention and would not fall within the scope of a "transaction" as recited in the claims of our application.

15. I hereby state that all statements made herein based on my own personal knowledge are true and correct and that all statements based on my information and belief are true and correct to the best of my knowledge, and further that all of these statements have been made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the present application.

24 September 2010
Date

Charles William Debney